Cabinet Office

OIX OPEN IDENTITY EXCHANGE

TOWARDS AN ARCHITECTURE FOR A DIGITAL BLUE BADGE SERVICE

The findings of an Alpha Project involving

Warwickshire County Council

GDS

DWP

innovate identity
experts in id

verizon

northgate PUBLIC SERVICES

mydex

White Paper

By Ian Litton and Rob Laurence

Executive Summary

The Government Digital Strategy sets out how the UK government will redesign its digital services so well that people will prefer to use them. The Digital Strategy deals with the transformation in the delivery of public services, with "digital by default" becoming the mantra. Initially aimed at central government departments and executive agencies, this mantra is now extending to local government, the NHS and elsewhere. The Digital Strategy is about modernising government, making use of digital channels and offering citizens a much improved experience when interacting with government whilst, at the same time, driving down the cost of delivery to the tax payer.

In this Alpha project we took a typical local government service – applying for a disabled parking badge (a Blue Badge) – and demonstrated how it could be radically transformed from a process taking several weeks to one taking a few minutes.

This was achieved through attribute exchange, defined as *"the online, real-time exchange of data specific to the transaction in hand, with the user present and with their full knowledge and permission"*.

The Alpha project involved the public and private sectors collaborating to design and build a working prototype of an attribute exchange solution. It was based on open source software and standards and completed in quick time with no material challenges arising.

The attribute exchange solution was underpinned by GOV.UK Verify, the government's identity assurance solution, thus ensuring that the identity of the user was known and trusted by the two parties in the attribute exchange process. This allowed the user to be part of the process and give explicit consent for data to be shared between the attribute provider and the relying party, thus enabling the transaction to be completed online and in real time.

Attribute exchange has the potential to deliver significant savings. At a DCLG Local Digital co-design event in July 2014 it was estimated that £100m could be saved each year by local authorities if they had access to Driver and Vehicle Licensing Agency (DVLA) data to deliver a range of services online, such as concessionary bus travel, taxi licences and parking permits.

If the 324 local planning authorities in England had access to Land Registry property data a saving of £97m could be made each year through fraud reduction and efficiency gains.

Attribute exchange has the potential to make an important contribution to realising the Government Digital Strategy. Verify and attribute exchange together can enable complex, eligibility-based services to be delivered as digital transactions.

OIX projects – demonstrating the value of collaboration

Despite the advancement of online services across the public and private sectors, hundreds of millions of transactions are still conducted using manual, face-to-face and telephone processes. Online identity assurance and the provision of verified attributes, together have huge potential to transform this picture into a truly digital landscape.

Transformation of this magnitude needs collaboration across sectors and industries, and a willingness to find common solutions. The open standards approach to identity assurance and attribute exchange, demonstrated in this OIX Alpha project, is one such example of how collaboration between the public and private sectors can underpin this transformation and achievement alignment of goals.

This white paper describes how the project team set about the design of the attribute exchange service and gives a high-level technical description of the solution built.

The paper also sets out the findings from three rounds of user experience research. This research showed that there are some real design challenges to consider, but fundamentally demonstrated that users understood attribute exchange and welcomed the opportunity to complete a complex transaction online.

The Alpha project builds on the findings of the preceding Discovery project. [1]

Transforming the Blue Badge Service with attribute exchange

This Alpha project focussed primarily on the Blue Badge application process for the 40% of holders (c. 160,000 disabled people annually) whose eligibility can be proven through the sharing of verified attributes between central and local government. For this segment an attribute exchange solution would be relatively straightforward to implement leading to a much-improved user experience.

For the remaining 60% (c. 240,000 people) a different form of data sharing and attribute exchange is required. Questions have been raised within this paper that will need to be addressed in subsequent Discovery and Alpha projects.

[1] See http://oixuk.org/wp-content/uploads/2014/09/WCC-2-white-paper-FINAL.pdf

Background and context

Table of Contents

In 2014, Warwickshire County Council, Government Digital Service, Mydex and Verizon collaborated in an OIX UK Discovery Project to digitise the Blue Badge transaction using a generic approach that could be applied to many locally delivered public services.

The Discovery project took the Blue Badge application as the principal use case and looked at how eligibility could be proven through Yes/No attribute confirmation in real time. Such a journey took 10 minutes and could lead to the applicant being in receipt of the badge within a few days rather than several weeks as at present. The findings were presented in the project white paper.

The conclusions reached indicated:

(a) there was strong user support for such an approach;
(b) local authorities and government attribute providers would gain from vastly improved performance and, at the same time, drive down the cost of service delivery;
(c) a new and significant market opportunity could emerge for the IT suppliers and private sector attribute providers.

Following the Discovery project, OIX commissioned an Alpha project with two specific objectives.

The first was to design and build a technical solution for attribute exchange, underpinned by the GOV.UK Verify service.

The second to carry out further user research, based on the Blue Badge application and incorporating the capture of an ID photo and payment.

In this white paper we report back on the findings of this project.

What we mean by attribute exchange

Definition and description

Within this project attribute exchange is defined as *"the online, real-time exchange of data specific to the transaction in hand, with the verified user present and with their full knowledge and permission"***.**

There are some key elements to this definition:

Online and real-time. This meets the requirement for digital by default, giving the user the opportunity to complete transactions online and in real time.

Specific to the transaction in hand. This meets the data minimisation principle embedded in the Data Protection Act by ensuring that only the data required for the transaction is exchanged. This in turn builds user trust and acceptance.

Verified user present. The user, whose identity has been verified to Level of Assurance 2[2], is present during the transaction and can assist the process if required. For example, to provide additional information that might assist user account or record matching with either the relying party or attribute provider.

User's full knowledge and permission. With the user online and present in the transaction explicit permission can be sought to share their data. Crucially, this avoids the need for complex data sharing agreements between organisations that can take years to negotiate.[3] Users who do not wish to give permission can be offered alternative means to obtain the service based on traditional channels.

Different types of attributes

The technical design for the digitalisation of the Blue Badge service considered three types of attributes:

- Identity attributes. These are the attributes provided by the identity provider through Verify that are used to match the user with a "user account" or database within a relying party or attribute provider. Such attributes include name, address, date of birth and gender. It was recognised that other sources of these attributes could exist; however, the basis of this design model is that Verify underpins attribute exchange.
- Confirmation (or predicated) attributes, ie YES/NO answers to status questions. For example, is this person over the age of 18? Is this person entitled to a blue badge?
- "Text" or "Value" attributes. For example, what benefits is this person in receipt of? What is the value of those benefits?

Although only the first two applied to the Blue Badge use case, the resulting technical design was intended to handle all three.

---

[2] LoA 2 is the level of assurance provided by Verify. It is a level of assurance that would stand up in a civil court, and confirms - on the balance of probabilities - that the person so assured is who they say they are.

[3] The highly regarded and successful Connect Digitally project implemented an online eligibility hub for free school meals. The data sharing agreements with DoE, DWP, HMRC and the Home Office took 2 years to negotiate.

In addition to these, other types of attributes exist. Biometrics, photographs and location are examples. But what about documents such as a patient's medical record or a clinician's assessment of a medical condition? Could and should these be included within an attribute exchange mechanism? These were outside the immediate scope of this project and the technical solution but need to be addressed in the wider context going forward.

Personal Data Stores as a source of attributes

Traditionally data about individuals has been collected, held and controlled by organisations. An alternative model – Personal Data Stores or Personal Information Brokers – turns this around and gives the individual control over their data.

The individual controls who can access their Personal Data Store (PDS) and what they can do with the information shared. The PDS is extensible and can hold a wide variety of information from detailed transaction records from utility companies, to health records, to signed and verified entitlements provided by accredited organisations.

Appendix A discusses Personal Data Stores as a source of attributes and encrypted documents.

Technical solution

The starting point for the technical design for the Alpha attribute exchange hub was taken from the findings of the preceding Discovery project.

These findings included

(a) user research
(b) design principles
(c) options for the high-level technical architecture

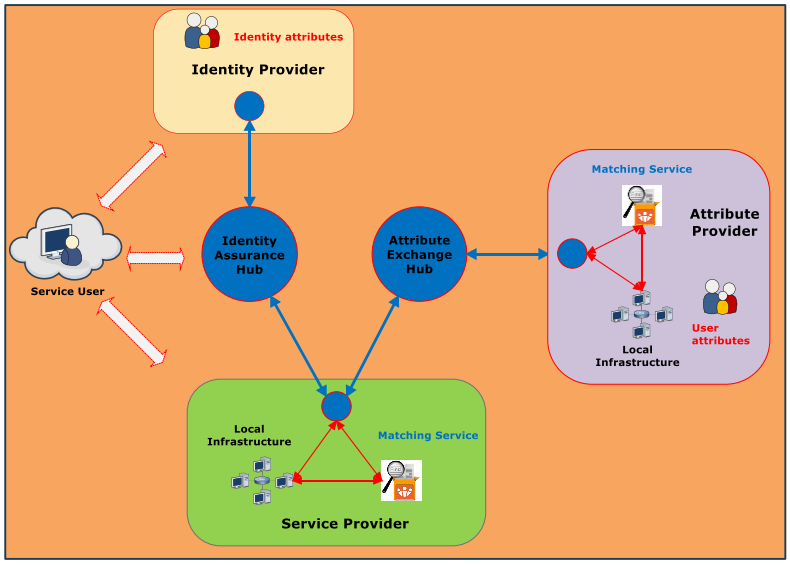
The Discovery project set out 3 potential designs for attribute exchange:

1. A combined identity assurance and attribute exchange hub
2. Separate identity assurance and attribute exchange hubs with attributes passing through the attribute exchange hub
3. Separate identity assurance and attribute exchange hubs with attributes passing directly from the attribute provider to the service provider

The project team designed the attribute exchange hub based on option 2 (shown in the schematic below). This was selected for a number of reasons:

- identity assurance has already been designed and developed as a common capability within the government platform

- identity assurance and attribute exchange can be treated as separate “services”, each simpler in its own right and each able to develop at its own speed
- sending all of the messaging via the hub, rather than point to point between service providers and attribute providers, simplifies on-boarding, and provides a consistent point for logging, auditing and billing. It better meets a number of the design principles established in the Discovery project



High-level technical architecture selected for Alpha project

At a high level, the attribute exchange hub designed for this project

- accepts an attribute request together with the identity attributes of the user that the service provider (ie relying party) passes through from the identity assurance hub (these are contained within the matching data set)
- checks that both the service provider and attribute provider are parties to the governing trust framework and the request is legitimate
- determines whether the user has given permission for the data to be shared, that is attribute(s) to be exchanged
- asks the attribute provider to approve the request and confirm it can locate the attribute for the user
- receives the attribute from the attribute provider and returns it to the service provider
- manages all aspects of security including the issuing and accepting of tokens and the encryption and decryption of messages in transit

Much care was taken by the project team to design the attribute exchange hub in such a way that it forms the basis of a platform that can be developed and enhanced to include future requirements as envisaged by the team. These were derived from the design principles, future potential needs, privacy guidance and potential technical constraints, as part of the design process.

The design was based on the existing and well established open standard, OAuth2. Emerging protocols, such as User-Managed Access (UMA) being developed by the Kantara Initiative organisation, were considered to not be sufficiently mature at the time of the Alpha build.

A full description of the technical design can be found in the associated document: *A Technical Design for a Blue Badge Digital Service – an OIX Alpha Project.*

Building and testing

The attribute exchange hub was built by Verizon, employing open source authentication software provided by ForgeRock.

Warwickshire County Council built the service provider interface to the hub.

Verizon built the two services that reside within the attribute provider domain: the authorisation service and the attribute service.

The build phase was completed within 4 weeks and end-to-end testing was accomplished within a further week with minimal issues.

The speed at which this phase of the project was completed reflects the thoroughness of the design process, which took place over a period of 13 weeks and involved the participation of architects and security experts from Mydex, GDS and DWP. The design was independently reviewed by the OIX Industry Working Group on Attribute Exchange and private-sector organisations.

The testing successfully demonstrated that:

- Messages requesting attributes originating from the service provider were received by the attribute exchange hub
- The hub was able to process these messages and broker the attribute request between the service provider and the attribute provider
- The two components with the attribute provider domain – the authorisation service and the attribute service – interoperated as intended
- Key security features such as encryption and token exchange were correctly implemented and enabled a secure attribute exchange service

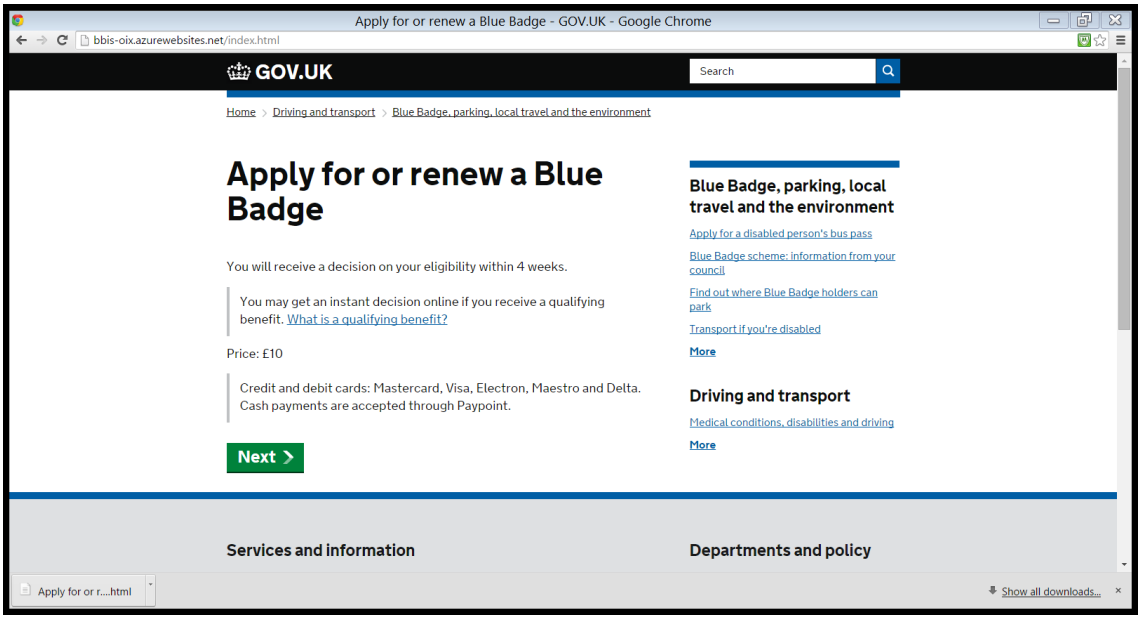
User research and findings

In the preceding Discovery project, user testing was performed using a prototype designed as a Warwickshire County Council online service, with a link to GOV.UK Verify to obtain assured digital identity credentials. Blue Badge eligibility checks were confirmed in real time with a notional Department for Work and Pensions (DWP) endpoint and vehicle checks with the DVLA endpoint. Users found the journey straightforward and there was a clear "wow" factor – genuine excitement from the users.

In this Alpha project the Blue Badge prototype was designed and styled as a GOV.UK service. The user journey was extended to include payment and capture of a digital ID photo. User research was carried out using a prototype built by Northgate Public Services, the current provider of the Blue Badge service commissioned for local authorities by the Department for Transport (DfT). The research was carried out over 3 days, each comprising 6 user sessions. Enough time was scheduled between research days to enable changes to be applied to the prototype if required.

The principal steps in the user journey are set out below, together with a description of the step and users' reactions.

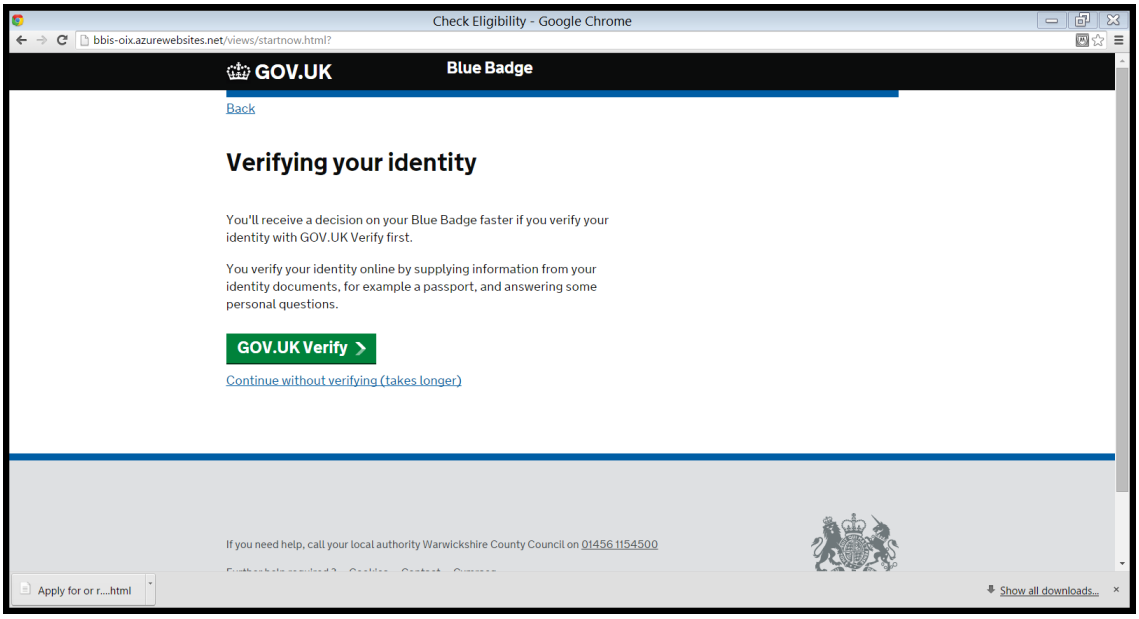
Step 1. Welcome and context setting
This screen is where the user journey starts. The user is made aware that a payment will be required. The next screen (not shown) informs the user that an ID photo will also be required.



User reactions. The natural inclination of most users was first to click on the link on the right of the screen to find out more about the Blue Badge scheme before proceeding with the application. They automatically went for "trigger" words such as "Council" and "Blue Badge". The large "Next" button at the bottom of the page was not a clear enough call to

Step 2. Verification of identity

Before the Blue Badge application process can commence the user is required to identify themselves through Verify. This screen leads to the Verify Registration or Sign-in screen (not shown).

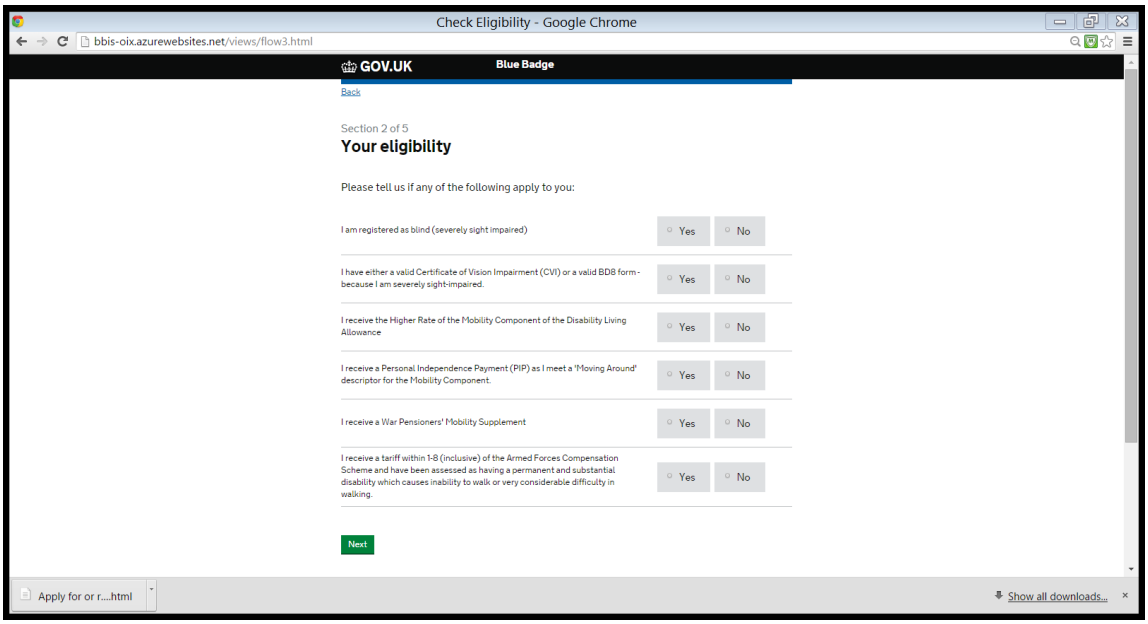


User reactions. While respondents understood the need for the eligibility of applicants to be checked, so that Blue Badges were not obtained fraudulently, the role of GOV.UK Verify in this process was often unclear (among those respondents who went through registration). Most users who were taken through the registration process were accepting of the practice of using documents such as the passport and driving licence as a means of identity verification. Knowledge based authentication, however, using financial information as a means of anti-impersonation checks, was confusing and many respondents had problems in associating this with the identity checking process. One user thought this was a way to obtain a credit record, which they welcomed! Another user thought they were being means-tested in relation to the £10 fee for a Blue Badge.

Users who were asked to imagine they had previously registered for an “identity account” and were asked to sign-in had no such problems and completely understood what was happening and why. Verify gave some respondents a feeling that their information was more secure; but for others it was a source of anxiety, particularly in relation to the perceived requirement for them to provide financial information.

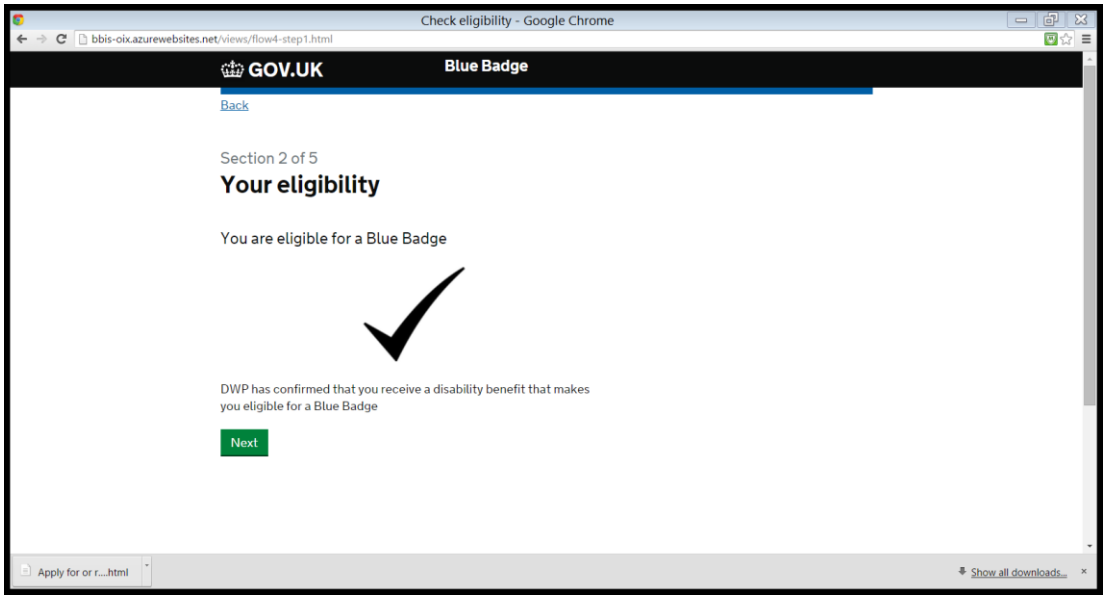
Step 3. Capture of eligibility criteria

Users who can answer “Yes” to one or more of these eligibility questions automatically qualify for a Blue Badge. On clicking <Next> the user is presented with a panel that asks for their permission for this eligibility to be checked with DWP (not shown). On giving permission the attribute exchange process is enacted through the attribute exchange hub.



User reactions. Most respondents were entirely comfortable with providing this information and giving their permission for their eligibility details to be checked. They recognised that this was to prevent fraudulent applications and welcomed this. Some users happily recounted situations where they had witnessed a Blue Badge being used fraudulently, and approved of measures being taken to prevent this. Other respondents however were unhappy with the act of giving permission. For one this was because of anxiety about Verify – she perceived that the attribute exchange permission would signal her assent to the Verify process, with which she was uncomfortable. For others the permission request seemed unnecessary and onerous – one more click in a long journey (made long by Verify registration, among other things). These findings show the potential vulnerability of attribute exchange: user acceptance of it can be affected by the context in which it is encountered.

Step 4. Confirmation of eligibility with DWP
The attribute exchange process takes place and confirmation is obtained from the DWP that the eligibility criteria is correct.

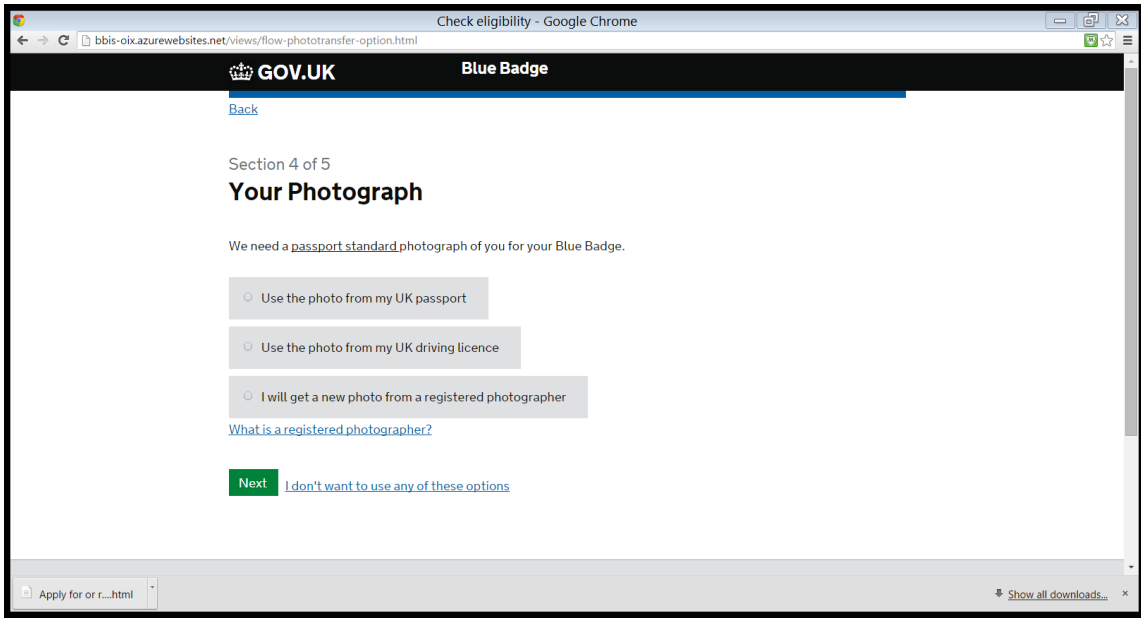


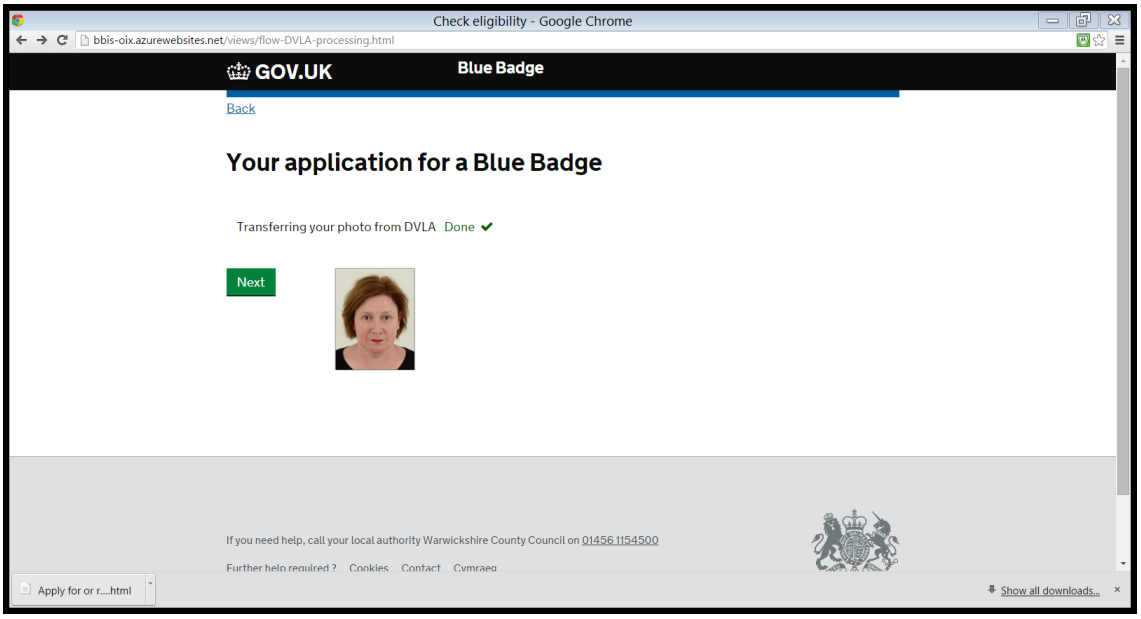
User reactions. Users understood the checks taking place and generally thought "that was good".

Step 5. Obtain a digital ID photograph

The user needs to provide a digital ID photo. In the user journey 3 options were provided with users being given the choice of which option to choose. In the prototype the driving licence option is enabled and permission is sought (not shown) to obtain their photo from the DVLA.

The photo is obtained using the attribute exchange hub and displayed to the user.

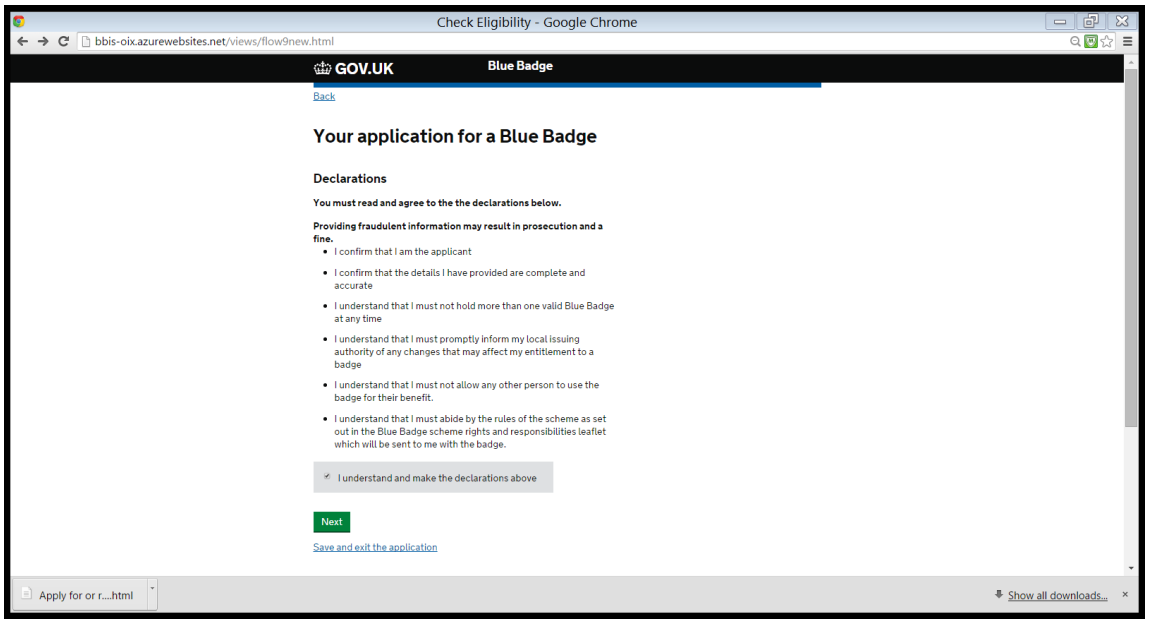




User reactions. Respondents who obtained their photo from their passport or driving licence were generally clear about and happy with the photographic part of the journey. Those who opted to obtain a new photograph from a registered photographer were much less happy – because the latter route was much harder to understand and seemed more onerous (particularly for respondents who had health or mobility problems.) Respondents who opted for the driving licence/passport route were generally happy to give permission for the photo to be obtained in real time from these sources (although, again, some felt that this permissions request was unnecessary). Being able to see the transferred photo drew positive reactions and comments.

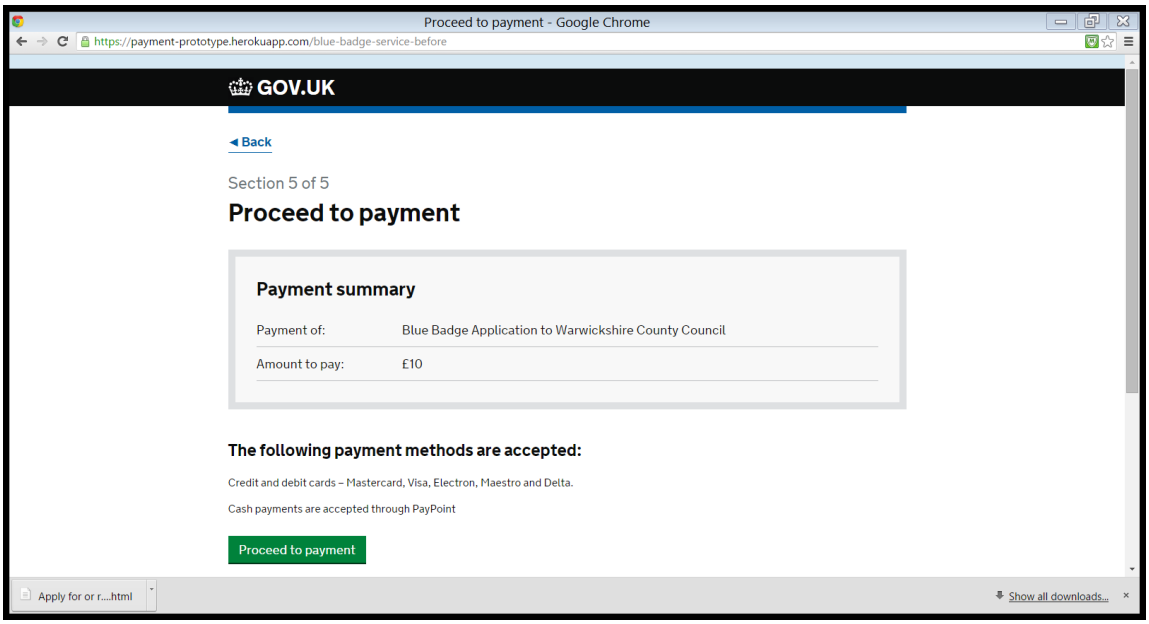
Step 6. Declaration

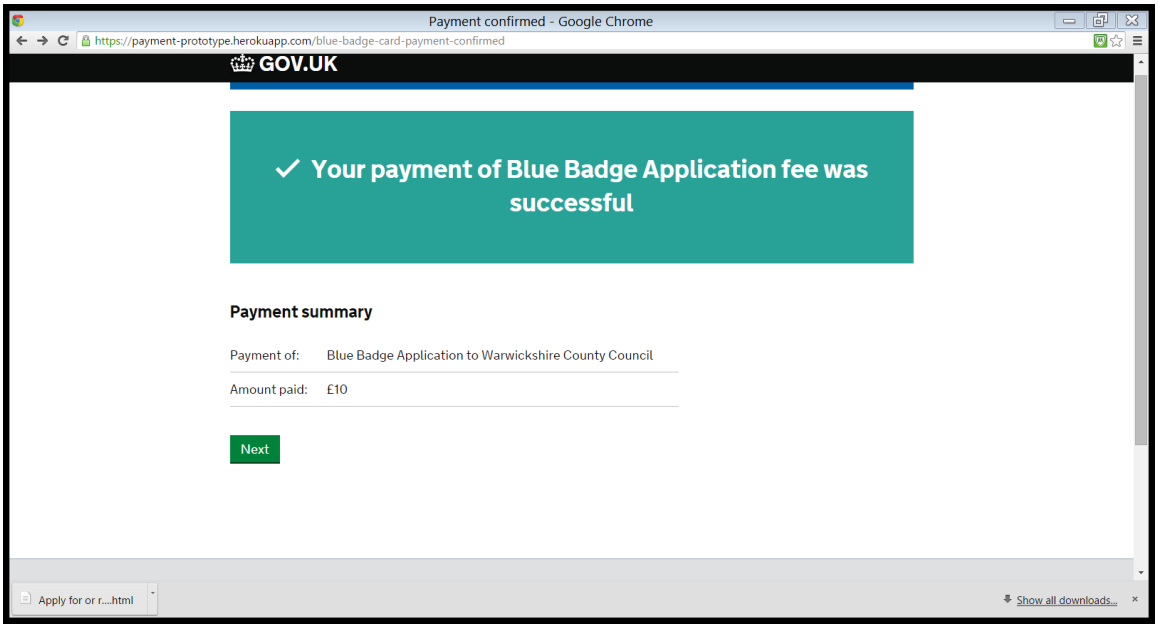
The user is required to declare that they understand what constitutes a fraudulent application and the consequences of making such an application.



User reactions. Most respondents expressed no objection to the presence of the declarations (with the exception of one, for whom they were over-long and unnecessary); and for some they were a welcome additional anti-fraud procedure. The declarations were read with varying degrees of attention by respondents – some gave them a close reading while others gave them just a very cursory inspection.

Step 7. Proceed to payment and finish
To complete the application a payment of £10 is required. Several payment options are available. The user is required to enter their chosen payment option and details as part of a typical online payment process (not shown).





User reactions. All users were familiar with online payments, although some may ask family members to make payments on their behalf. All selected the debit/credit card option. No users were familiar with the PayPoint option, perhaps reflecting the demographic used for the research.

The principal findings from the three days of user research were as follows.

1. With both Verify and the Blue Badge following the GOV.UK style guidance there were few visual clues that these were different services. Users found this confusing and had trouble in describing where they were in the journey. As the prototype evolved clearer descriptions and "signposting" were introduced within pages and on clickable action buttons. This improved the user experience but still the impression was that more was needed.

2. Although the primary aim was to test users' views on attribute exchange it was realised that this couldn't be achieved in isolation to the GOV.UK Verify component of the user journey. Verify and registering for an identity account raised numerous issues that impacted negatively on users' views of the complete journey. Where users were asked to simply sign-in to an existing identity account views were much more positive about their experience.

3. The first version of the prototype involved obtaining a digital ID photo from a photographer and then coming back to the online service to complete the application. This was disliked by many with several users suggesting that the process should end with the photographer. This process was changed for the last round of testing and seemed to be better received, though it was not possible to test this extensively (see highlighted panel below - Obtaining a Digital ID Photo). However, there was still a strong preference for obtaining the photograph from the Passport Office or the DVLA by attribute exchange.

4. Users found the Blue Badge application part of the user journey very straightforward, variously describing it as "a good idea, "it was easy" and "simplicity itself". Users welcomed the benefits that a digital service brings over the existing paper application process, saying that it was "quicker and less hassle".

Obtaining a digital ID photo

The user was presented with two options to provide a digital ID photo. The first involved using an existing passport or driving licence photo. The second involved the user visiting an approved photographer.

If the user selected the first option the photo was obtained digitally using the principles of attribute exchange. Most users viewed this as very simple and easy, as one user put it: “Simplicity in itself!”.

In the second option the user was presented with a list of approved photographers in the proximity of a given postcode. At this point in the journey the user was asked to print a unique QR code to take when obtaining a photo. From the user research perspective, the journey ended at this point. For the sake of understanding, it is envisaged that the following steps would subsequently take place.

The QR code, which identifies the Blue Badge application, would be scanned at the point of obtaining the photo and automatically link the photo to the Blue Badge application. The photographic service would forward the photo and identifiers to a Blue Badge temporary photo store. The Blue Badge service would then retrieve the photo and forward the completed application to the relevant local authority for approval.

Overall, users generally felt that obtaining a photo from their passport or driving licence was a straightforward process. Most would opt for this rather than have to visit an approved photographer or booth.

Conclusions and recommendations

This project set out with two specific aims. The first was to design and develop a technical solution for attribute exchange. The second to conduct further research to understand users’ views on the use of attribute exchange across government to enable the delivery of complex transactions such as the Blue Badge service.

The conclusions drawn are as follows.

1. It was technically straightforward to build a working attribute exchange solution based on an open authorisation protocol (OAuth2) and open source software provided and supported by ForgeRock.

2. Although this was an Alpha project it was a strong wish of the participants, who were investing their time and resources, to create an open standards based approach to attribute exchange that works across the public and private sectors. The design of the attribute exchange solution reflects this and is capable of handling different types of attributes and is extendable to include future anticipated requirements. Issues such as matching a user's identity attributes with those held by an attribute provider, or where an attribute provider may require a higher level of assurance of the user's identity, were addressed in the design concept. Overall, the participants' view is that this is a design that can be taken forward within future projects involving attribute exchange.

3. The findings of the user research indicated further specialist design work is needed to the user journey. Generally, the users were somewhat "matter of fact" about their experience, happy to say that the attribute exchange driven online Blue Badge application was a good idea but, tellingly, unable to articulate their understanding of the overall journey accurately. This was particularly evident when undertaking registration for an identity account and the knowledge based authentication cycle.

Set out below are recommendations on areas that should be explored further, either within subsequent projects or as part of an industry-wide initiative. Some of these are driven by the opportunity to redesign the Blue Badge application process as a fully online service.

1. Develop the user journey prototype to incorporate a number of improvements resulting from the findings of the user research. These include improving the start page, better signposting of where the user is within the journey, and better differentiation of the Verify process and the Blue Badge application process.

2. Working with private-sector technology companies, further develop the prototype attribute exchange hub into a full production platform. This would include provision for

    a. the handling and translation of various "open" protocols adopted by service providers and attribute providers
    b. a standardised approach to defining attributes and their sources (an attribute data dictionary)
    c. the implementation of a trust framework for attribute exchange including commercial models
    d. logging requests and access; billing and auditing
    e. alternative forms of attribute exchange as described in this white paper

3. Incorporate the attribute exchange hub into the test identity infrastructure being developed by OIX and re-use within other projects requiring user-permissioned data sharing.

4. Investigate the technical capabilities of the photo booth and the interaction with the user. Determine whether the user can scan codes or input data within the booth and understand how straightforward and acceptable this would be.

5. Engage the Privacy and Consumer Advisory Group (PCAG) to consider the identity principles in the context of attribute exchange.

6. Address the need for the identity assurance hub to become the trust anchor for user identity tokens consumed within the attribute exchange network. This requires further development of the GOV.UK identity assurance hub or for a private supplier to provide an equivalent service.

Undertaking these recommendations could quickly lead towards

- transformation of the Blue Badge service for the 40% of holders who qualify through fast-track verifiable eligibility criteria
- investigation into finding an approach for the remaining 60% who qualify on the basis of supporting and corroborating evidence
- the delivery of a complex local government service as an “exemplar” demonstration of the power of attribute exchange.

Such a project would signpost the way to transform around 50 additional local government services that could benefit from attribute exchange. There are many more central government and private sector transactions that could similarly benefit.

Appendix A – Personal Data Stores as a source of attributes

This project focused specifically on building a technical solution to support predicated YES/NO attribute exchange. In reaching a technical solution the design team also considered the extensibility of the solution to meet other forms of attribute exchange.

The Blue Badge is an interesting and complex use case to explore further. As is highlighted in this white paper, this project addressed a segment of Blue Badge holders whose eligibility could be confirmed through an exchange of attributes with the DWP. The technical solution delivered this capability.

There is a larger segment, though, who need to provide an objective assessment of the extent of their disability. This needs to be corroborated by documentary evidence from, say, an independent mobility expert. (Approximately two thirds of this segment are currently able to provide this with the remainder having to attend face-to-face assessments with their local authority).

This segment, therefore, provides both a procedural and technical challenge to address and resolve if the Blue Badge application process is to be fully transformed for the vast majority of applicants.

Many questions arise which require investigation and are outside the scope of this project.

Could attribute exchange be extended to include document exchange?

How could trust be established in both the provider and holder of the attributes or documents?

Could personal data stores potentially be part of the solution?

The Citizen's Advice Bureau (CAB) Report, *Personal data empowerment: time for a fairer data deal?*[4] sets out strongly the case for person-centred data sharing in all its forms. Much of the findings of the user research in this Alpha project mirror those in the CAB report. The report could provide valuable input into the next phase of research.

The Policy Exchange report, *Small Pieces Loosely Joined*[5], also sets out the case for individuals to manage their own data through personal data stores.

"Ultimately, government must trust individuals to manage their own data through personal data stores. It should commit to public sector-wide compatibility with personal data stores

[4] See https://www.citizensadvice.org.uk/about-us/policy/policy-research-topics/consumer-policy-research/personal-data-empowerment-time-for-a-fairer-deal/

[5] See http://www.policyexchange.org.uk/images/publications/small%20pieces%20loosely%20joined.pdf

(PDS) that allow individuals to choose which public sector organisations see their data and for how long. The market is currently embryonic, but with a strong commitment from the public sector to embrace the model, it could be expanded rapidly. This would be the logical extension of the GOV.UK Verify programme, which allows citizens to prove their identity via a trusted third party, such as Verizon or Experian. There would be considerable benefits for both the public sector and citizens from adopting PDS."

Glossary

assured identity	An identity that has been verified to the required level of assurance by an identity provider
attributes	The personal information provided by a principal that's to be authenticated by the identity provider Data linked or about an Identity that support and/or indicate such things as entitlement, authority, right to work
attribute enrichment	The onward use of attributes delivered as part of the identity assurance process. The service provider will either use them in a user journey they are accessing or use it to populate a user record within the service provider records.
attribute exchange	The request for, authorisation and sending of an attribute, or attributes, originating from a relying party to an attribute provider.
attribute provider	An entity that can assert attribute values in line with the policies set by the scheme it is being used within. It responds to a request from a trusted relying party.
attribute provision	A generic term to cover both attribute enrichment and attribute exchange.
data matching	The process of finding a local identifier through matching that is useful to the relying party when completing a transaction. For example, confirming a National Insurance number so the principal can amend their tax records
Data Protection Act 1998 (DPA)	A piece of UK legislation covering the processing, transporting and storing of personal data
digital identity	The digital representation of an entity that's authenticated through the use of a credential
Government Digital Service (GDS)	The organisation within the Cabinet Office with the responsibility for transforming government and Identity Assurance
hub (identity assurance hub)	The website that manages communications between users, relying parties and identity providers for the purpose of authentication to a service operating in a federated identity system.

	It provides a clear divide between the identity providers and service providers, avoiding complex many-many integration between identity and service providers. It also ensures privacy and security during authentication transactions.
identity	The attributes of a person that make them unique from other people; who a person is In the case of identity assurance, this is the description of being who or what an entity is, defined by a collection of attributes
identity assurance	The ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity . Proving you are who you say you are to a certain level of 'trust'
identity provider (IDP)	Private sector organisations paid by the government to verify a user is who they say they are and assert verified data that uniquely identifies them to the relying party The organisations are certified as meeting relevant industry security standards and identity assurance standards published by the Cabinet Office and CESG (the UK's national technical authority). Also called a certified company Holder of the source of authority database to which a credential is bound and managed
matching service (MS)	The service that matches data from the identity provider to the transaction's local data store in order to tie the principal's identity to their transaction account
matching data set (MDS)	The minimum data set of name, address, date of birth and gender sent by the identity provider to the relying party matching service for the purpose of matching
Open Identity Exchange	A non-profit trade organisation of market leaders from competing business sectors driving the expansion of existing online services and the adoption of new online products. Business sectors include the internet (Google, PayPal), data aggregation (Equifax, Experian) and telecommunications (AT&T, Verizon)
personal data	Data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

	and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
personal details	A combination of personal name and at least 1 of date of birth or address. Not to be confused with personal data as defined by the Data Protection Act
principal	The person whose identity is being assured
Privacy and Consumer Advisory Group	Established to help the government develop an approach to identity assurance and come up with the Identity Assurance Principles
privacy principles	A set of principles set by the Privacy and Consumer Advisory Group that aim to protect an individual's privacy when using identity assurance
relying party (RP)	A government service, such as HMRC or DVLA, that needs proof of a person's identity to complete a transaction. In SAML specifications, a relying party is a system entity that depends on receiving assertions from an asserting party (a SAML authority) about a subject, eg an assertion of identity from an identity provider
SAML (Security Assertion Markup Language)	An Extensible Markup Language (XML) open standard for the exchange of authentication and authorisation data between parties such as identity providers and relying parties., The SAML standards are governed by OASIS. A SAML Profile derived from core SAML standards is used for the purposes of signing in to government services under identity assurance. Created by OASIS
service provider (SP)	Provide government services to users. Service providers are referred to as 'relying parties' to avoid confusion between those providing the government service to the user and those providing the identity service to the user
sign in	The name for the process of using identity assurance to access digital transactions on GOV.UK
single sign-on	A user's single authentication ticket, or token, is trusted across multiple IT systems or even organisations
standards	The quality levels that need to be met by the identity providers and specifications that they should be compliant with

transaction	The thing the user wants to do or get from a government service. An individual online service that a government service offers, eg renew a passport
user journey	The steps a user takes to complete a task within the hub
user	The person accessing the government or local government service. Not necessarily the same as the principal, eg could be a carer filling in a form on behalf of the person that they care for